THE NEW STANDARD FOR CYBER SECURITY

Cameron Shearon
MA, USA
Cameron@Shearon-Consulting.com

ABSTRACT
Historically, Cyber Security has been limited to software. Because of IPC 1782, IPC 2581, and IPC 2591, it is possible to know exactly what hardware is in any electronic device. Therefore, hardware can be part of the Cyber Security solution. In addition, by coupling the hardware and software Cyber Security approaches with the Framework for End to End in Situ Monitoring described in Section 9.5 of ETSI GS NFV-REL 004 V1.1.1 (2016-04), a comprehensive Cyber Security solution can be created.

Implementing IPC 1782, IPC 2581, and IPC 2591 with a very innovative labeling system within a factory and across the Supply Chain will increase yields, improve Quality, and Improve Reliability, as well as, make these items much more predictable. In addition to productivity gains, implementing these standards across the Supply Chain will fight counterfeits systematically. Because counterfeiters are opportunistic and operate in the "'dark" by surprise attacks, they are like guerilla fighters in a sense. The best way to deal with this type of "attack" is by taking a systematic approach and shining light, by sharing information, where there is currently darkness. Combining these three IPC standards with other technologies such as innovative tagging technologies, Blockchain, The Cloud, and Big Data Tools enable unprecedented productivity gains not seen since interchangeable parts enabled the Industrial Revolution, as well as, the ability to catch counterfeits in situ before the components go through the next process step in a factory. This can be done regardless of the path taken from the original manufacturing site to the next downstream manufacturer. The true beauty of this approach is that no single entity shoulders the cost of this solution.

Variability causes yield, quality, reliability (quality over time), and product safety issues. Interchangeable parts enabled the industrial revolution because they addressed variability. What gets measured tends to get managed. This combination of tools enables a tailorable solution that is proportionate to the need and available resources. Therefore, this solution fits very well with Smart Factory/Industry 4.0, materially increases productivity, and can be utilized to create entirely new business models, as well as, a practical way to address the risk of counterfeits and Cyber Security for a very long time.

Key words: Smart Factory, Industry 4.0, Smart Factory, Cyber Security, Traceability, Counterfeit

INTRODUCTION[i]

Despite considerable resources having been spent to ensure Cyber Security and that counterfeits do not enter the Supply Chain or end up in customer's hands, the solutions implemented have not been 100% effective & have been very expensive to implement & maintain. Moreover, as counterfeiters obtain more resources, the number of resources consumed to prevent issues will increase markedly and become increasing less effective. The most counterfeited electronic parts are capacitors and resistors. Cyber Security has only been focused on software up to this point. Because of how software is developed and tested, it is possible for Cyber Security threats to be implemented after the regression testing of that section has been completed. Also, part of the Cyber Security threat could be in the software and part of it in the hardware. This combination may be turned on in the field and not detected for a long time. It is difficult, if not impossible, using currently implemented technologies to ensure no counterfeits are utilized. It is even more difficult to ensure that the current Cyber Security solutions are sufficiently effective. One only has to look at the number of entities that have been hacked to see that this is correct. Because business moves at the speed of trust and most of the economic transactions occur on electronic devices and across networks, Cyber Security solutions need to be much more effective than the ones currently available. Why not utilize a systematic method that can be 100% effective and be a productivity tool too?

IPC-1782 Traceability Standard

Traditionally, traceability has meant tracking a package while it has been shipped or an analogous approach. Historically, there has not been a standard way to articulate the level of traceability or what exactly will be captured at each step in a manufacturing processes or perform traceability on individual electrical components (e.g.; integrated circuits, resistors, capacitors, etc.). IPC-1782 is the first traceability standard that solves that problem. Because of how IPC-1782 is structured, it can easily be tailored to other areas like mechanical items, food, medicine, implantable medical devices, and more.

From a technical perspective, traceability is a build record of a product which includes all of the process parameters, maintenance history of the equipment used to make that product, product information & flow data, the materials used to make that product, and variability within & across products. Targeting the causes of this variability will increase productivity, raise yield, and enable a better

allocation of resources within a factory & across an entire supply chain.

From a business perspective, traceability is a measurement of resource allocation, risk, supply chain issues, efficiency, productivity, Quality, Safety, minimizing the impact of recalls, Reliability, and enables flexibility.

Historically, traceability has been an all or nothing approach. Therefore, traceability has been very limited in its application (e.g.; specialized safety or reliability or quality needs).

IPC-1782 has four levels a traceability for Materials and four independent levels of Processes. This approach enables the right level of traceability to be applied based on the risk involved for that part.

Regardless of what system is used to measure risk, fundamentally, it is a combination of the likelihood of an event occurring and the impact of that event if it hypothetically were to occur. Everything that impacts the quality and reliability of the materials and processes of an SMT (Surface Mount Technology) or Circuit Card Assembly (CCA) operation is captured in IPC-1782. The principals and methodology of IPC-1782 can be applied to any industry (e.g. food, medicine, vehicles, appliances, etc.). IPC-1782 Level 1 measures the materials and processes at a 3σ level. IPC-1782 Level 2 measures the materials and processes at a 4σ level. IPC-1782 Level 3 measures the materials and processes at a 6σ level. IPC-1782 Level 4 measures the materials and processes at a 9σ level.

Because products have different failure mechanisms and different risks, each component of a product would need to be produced at a different level. As an example, keys on a notebook computer may only require Level 1 Traceability (3σ) and the battery of that same notebook computer may require Level 4 Traceability to ensure it does not vent with flame on a flying aircraft.

If everything was produced at a Level 3 Traceability (6σ), then resources would be wasted on the components such as the keys while thousands of notebook computer batteries would vent flame each year. Because a fundamental definition of intelligence is making the most of the available resources, then applying one level of Traceability to every component of a single product or of every product is not the smartest approach for an organization. Organizations are really editors of features that they expect their customers to value. Therefore, leveraging this approach will allow organizations to be better editors of features and better allocate resources.

IPC-1782 was developed with a modern approach to creating standards. To provide the most flexibility for a tailored solution and to make the standard the most useful to the broadest audiences over the longest period of time, IPC-1782 leverages an expandable and extendable data structure. This data structure can be adopted for all levels of traceability and enable easily exchanged information, as appropriate, across many industries & supply chains.
IPC-1782 can be applied to manual processes, as well as, fully automated processes and everything in between. Patterns in this data can be found using existing off the shelf modern analytical techniques that will be discussed later in this paper. IPC is now interested in expanding their standards to where the Electronics Industry had gone and not just limit its application to the Electronics Industry. This would enable applying this approach to mechanical parts, as well as, breaking down the traditional silos between the Electrical and Mechanical parts of an organization and their tools.

Capturing IPC-1782 data would enable material traceability, process traceability, exceptions, regulated substances, and process maintenance.

IPC-1782 establishes minimum requirements of manufacturing and supply chain traceability based on perceived risk As Agreed Between User and Supplier (AABUS). It applies to all products, processes, assemblies, parts, components, equipment used and other items as defined by user and suppliers in the manufacture of printed board assemblies. IPC-1782 establishes minimum requirements are based on four levels of traceability for materials and processes. This makes it easier to articulate in a contract and budget to implement in phases through time on a variety of products. These levels can correlate to the IPC Product Classification System (Class 1, Class 2, and Class 3) and/or another set of categories of compliance, based on the business model/economic needs of the end use market for the final product (e.g. telecom, aerospace, automotive, medical device, consumer electronics, etc.) or a subassembly within that product.

Table 1 shows how each IPC -1782 traceability level works. product classification maps in general against Traceability levels. Levels of material and process traceability need not be the same. Exceptions may be granted for additional or relaxed requirements as agreed for example, under contract

Table 1: IPC-1782 Traceability Levels

	Level 1: Basic	Level 2: Standard	Level 3: Advanced	Level 4: Comprehensive
Material Traceability	M1: Part number listed to work-order	M2: Unique material ID listed to work-order	M3: Unique material ID listed to PCBA	M4: Unique material ID listed to reference designator
Process Traceability	P1: List significant process exceptions to work-order	P2: List critical process characteristics and exceptions to serialized PCBA	P3: List all key process characteristics and exceptions to serialized PCBA	P4: Capture all available metrics to serialized PCBA
Data Integrity (in the range of)	3 Sigma 93.3%	4 Sigma 99.38%	6 Sigma 99.99966%	9 Sigma 99.99999999999999%
Data Collection/ Storage Automation	90 % Manual	70 % Automation	> 90 % Automation	Fully automated
Reporting Lead Time	48 hours	24 hours	1 shift	Available at completion of the process
Data Retention Time	Life of product plus 1 year	Life of product plus 3 years	Life of product plus 5 years	Life of product plus 7 years

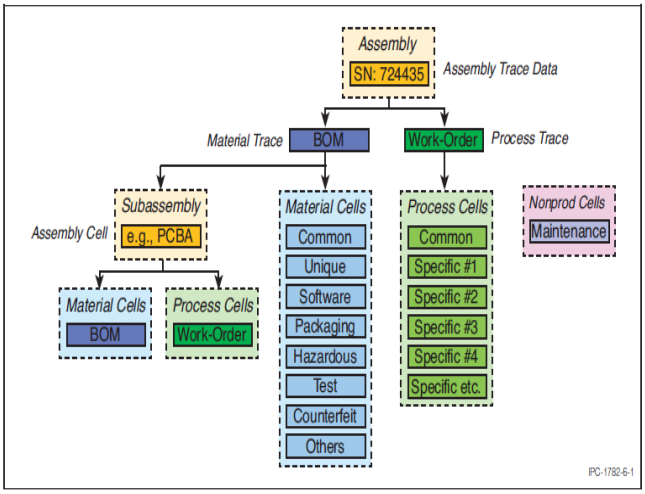

Figure 1: Data Structure of IPC-1782

When implementing IPC-1782, an organization needs to develop an End-To-End solution that anticipates or eliminates human error throughout the process and implements the tools, training, and appropriate resources to proactively find and manage problems. This should be based on risk. Because what gets measured tends to get managed, an organization measure the resources that need to be managed. The data should be contained in a single database rather than disparate databases. The data should be structured to find patterns in the data in the easiest and most productive way possible & be sustainable. This should be factored into your End-To-End Implementation Plan Of Action. Think in terms of completing a "Digital Build Record" or a "Digital Build Model" to encapsulate a complete set of records which include exact history, exceptions, specific materials used, complete maintenance records along with supplies utilized, process events, key process parameters, equipment used, daily checks, specific personnel responsible for the processes for that specific build, measurements from every relevant test and inspection, as well as, include a formal report for any defect investigation, disposition, and/or repair history. This information is crucial because people's memories are not perfect and fade over time. IPC is developing a "Digital Build Model" standard. Generating a flow diagram for each quantified work in progress will enable everyone to walk the process. This is a key part of any comprehensive Quality System. This would ideally be done automatically without human intervention utilizing the information already collected. Educate everyone in the organization about how to determine risk and make the appropriate risk versus reward decisions for your organization's culture and the industry in which you operate. This will empower line workers and make everyone in the organization better consumers of this information. This approach will enable the organization to function much more coherently as an organism. Set clear goals and expectations up front to ensure the entire organization works towards the same goal(s) from their various perspectives. This approach enables an organization to make the best use of diverse perspectives and make the organization the most productive possible. This negotiation and clarification step is also crucial to the entire global supply chain. If the entire supply chain follows the same approach and utilizes the same terminology, it makes it much easier to find and eliminate waste/problems much faster. Collection of and finding patterns in the data automatically enables machines to do what they do best and people to do what they do best. Thus, automating the data collection and analysis by implementing known pattern recognition will help everyone be more productive, as well as, have fewer human errors. This is also an opportunity to utilize augmented reality tools to help avoid mistakes in production and maintenance work. Mobile devices on the manufacturing flow that highlight problems automatically to the humans will also help catch and correct problems early. Utilizing a reporting tool that enables universally accessible information will make every stakeholder an advocate for the organization, the supply chain, and ultimately, the customer. This leads to a win-win-win scenario. Coupling this approach with the automation scenario will not only allow for near real-time analysis, it will facilitate predictive analytics to avoid problems rather than react to them after the damage is done.

Variability causes uncertainty, Quality, Reliability (Quality over Time), and Safety problems. IPC-1782 is a powerful tool to minimize the variability and uncertainty. Uncertainty causes fear. If properly implemented and utilized, IPC-1782 can effectively create and maintain trust with all stakeholders by making any organization utilizing it, much more in control of the inherent variability.

The reduction of uncertainty by implementing a proper component traceability program is on par with the reduction of uncertainty by using interchangeable parts that enabled the Industrial Revolution. This approach enables Industry 4.0 and a Smart Factory, as well as, a Smart Supply Chain.

IPC-1782 makes programs such as ISO 9000 and other quality management systems work much better. IPC-1782 does not replace these other quality management systems. It augments and supplements them if implemented properly.

Because IPC-1782 captures so much more information, an organization will be able to identify "one off" failures by implementing a systematic approach.

IPC-1782 can be utilized as a strong Anti-Counterfeit tool, and part of a comprehensive Cyber Security solution. This is especially true if an organization is buying components, materials, or services from gray market suppliers that are End of Life parts. Regulatory barriers are there to prevent organizations unexpectedly going out of business or unexpectedly stopping production due to unforeseen events.

IPC-1782 Component Traceability reduces the risk of counterfeit components, Cyber Security threats, improves quality, increases reliability, decreases costs, drives product innovation

IPC-2581 Digital Product Model[ii]

Transferring design data to the SMT/CCA line has historically required multiple files and interpretation of that information across multiple formats which create opportunities for errors, as well as, requiring excessive lead times and unnecessary work & costs to implement (see Figure 2). This approach can also lead to a loss of Intellectual Property, Counterfeits, and Cyber Security risks. IPC 2581 solves these problems by using a single file approach (see Figure 3), as well as, walls off any parts of that file that you do not want to expose to anyone that does not need to know.

IPC 2581 is a complete digital PCB product model contained in a single file. This single file contains design and local BOM data & variants, as well as, is ready for direct process engineering tasks.

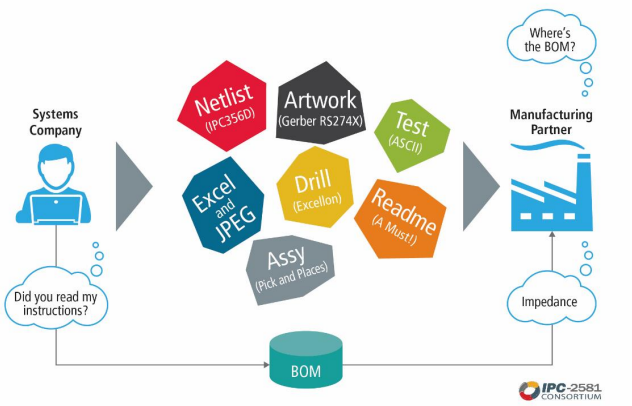

Figure 2: Prior Ways of Conveying Design Information

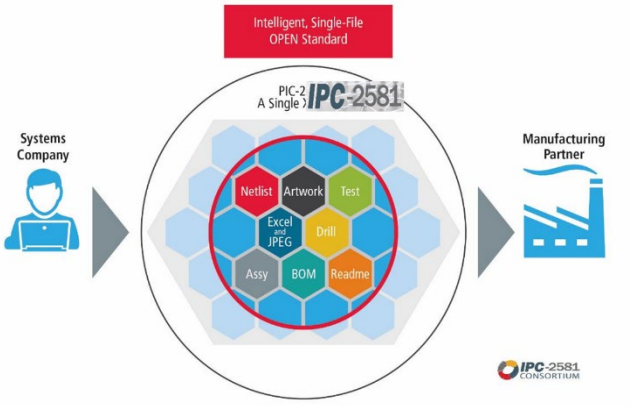

Figure 3: IPC 2581's Single File Approach

Figure 4 shows how various approaches compare. IPC-2581 has been successfully implemented for years by large multinational companies.

	Graphical Features	Feature Intelligence	Stackup	Mechanical Specification	Notes	Fabrication Acceptability Specification
RS-274X	√	Manually Added	ePaper Drawing	ePaper Drawing	ePaper Drawing	ePaper Documents
ODB++	√	√	ePaper Drawing	ePaper Drawing	ePaper Drawing	ePaper Documents
IPC-2581	√	√	√	√	√	ePaper Documents

Figure 4: How the various approaches compare

Unique Attributes:

IPC-2581 is the ONLY open, intelligent standard format available to the industry. It provides complete machine-readable data for all aspects of PCB manufacturing. This makes implementing the design faster, easier, and with fewer mistakes. IPC-2581 is the only standard that enables electronic stack up exchange. IPC-2581 has proven to improve product quality and first-pass success

Figure 5 shows the IPC-2581 digital flow of information and how it gets parsed along the way.

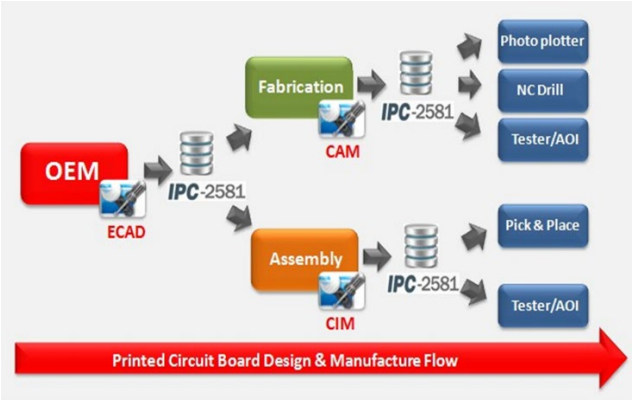

Figure 5: IPC 2581 Digital Flow

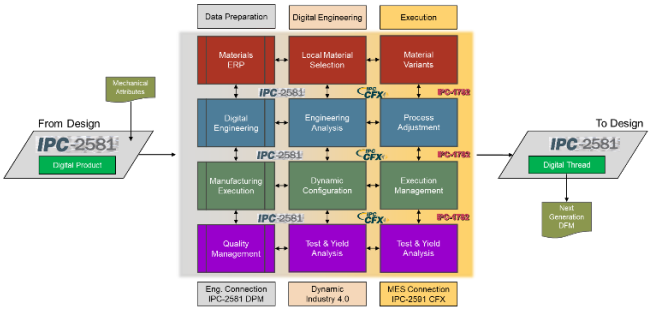

Figure 6: IPC Complete Digital Manufacturing "Closed Loop" Flow

Figure 6 shows the IPC-2581 "Closed Loop" flow. This complete digital manufacturing "Closed Loop" flow enables better conversations between Design and Manufacturing groups. This approach also enables a Design Of Experiment (DOE) approach over the entire process and factory.

IPC's CFX (Connected Factory Software Standard)
IPC-2591 (IPC's CFX; Connected Factory Exchange Standard) was created to pick up the IPC-1782 Traceability Information and enable the factory to be more productive.

Historically, each equipment supplier had their own communication standard. In some cases, equipment suppliers would not have a coherent communication approach across all of their products. Similar equipment would have different software builds and require an entirely different software driver for that particular piece of equipment. This has limited Circuit Card Assemblers and Surface Mounted Technology lines in finding patterns in their data. This limitation has limited their yield and productivity.

The IPC CFX Standard has brought together hundreds of vendors and solution providers working together. IPC-2591 is a genuine IIoT "plug and play" standard for Smart Factories. IPC's CFX is available free to companies of all sizes in all industries. Because of this easy to implement coherent approach, waste, variability and digital value creation are now possible.

Figure 7 shows how IPC's CFX Standard not only uses the same AMQP communication protocol as used for financial transactions, it also defines a common language content. If this standard did not have both approaches covered, then it would be like two people talking on a mobile phone while speaking different languages. If neither person understood the other's language, then there would not be any communication occurring.

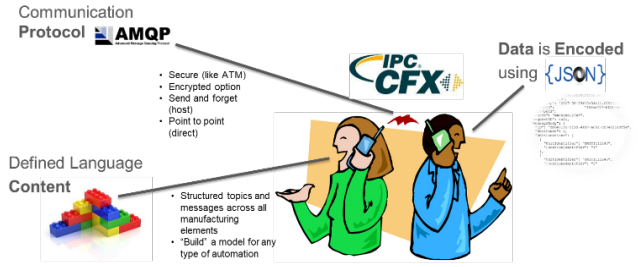

Figure 7: CFX Components For True Plug And Play

Figure 8 shows this language in part by showing some of the defined messages in the standard.

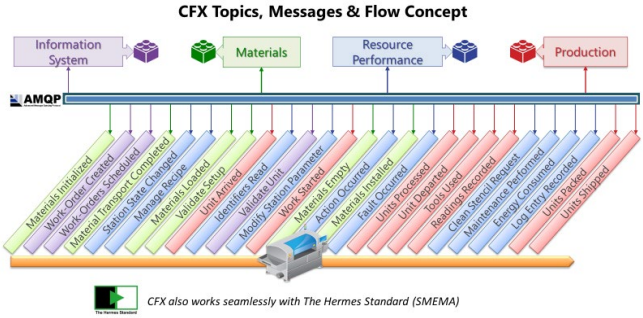

Figure 8: CFX Message Content Blocks

Hierarchy Of Data:
Because of the indexed hierarchy data structure that IPC's CFX uses, it reduces the data size, defines common data once, can be referenced as needed, and matches IPC-1782's structure which makes it easier to add data later.

Blockchain
Blockchain was created for Cryptocurrencies where there is no trust in the financial exchange. Also, the history is immutable.

In a sense, Blockchain is analogous to containers on a ship except these containers hold data that cannot be changed or modified and connect to the events before & after it..

Blockchain is a growing list of records, called blocks, linked using cryptography (See Figure 9).

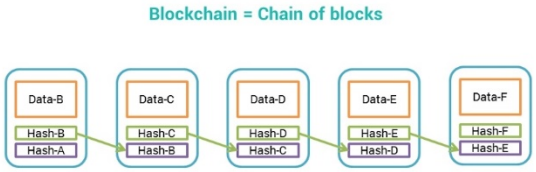

Figure 9: Shows how the blocks are connected by a unique key called a Hash

Attributes Of Blockchain:

- Assumes no trust
- Immutable: Once data is written, it cannot be changed
- The data inside the block becomes mathematically incorporated in the Hash which links the adjacent containers of data
- Not good for large blocks of data
- Blockchain divides data into a series of blocks, with pointers
- Many copies of each block exists
- When reading, all copies of all blocks are sewn back together, to ensure consistency

Industrial Internet of Things (IIOT)

The industrial internet of things (IIoT) extends the use of Internet Of Things (IOT) into Industrial Sectors and applications. IIOT is about connecting everything to measure cause & effect and be proactive about solving problems. In addition, IIOT helps clarify how consumers use products. This enables better designs and features in future products, services, and solutions.

Figure 10 shows some of the things that can be connected.

Figure 10: Some of the things currently being connected.

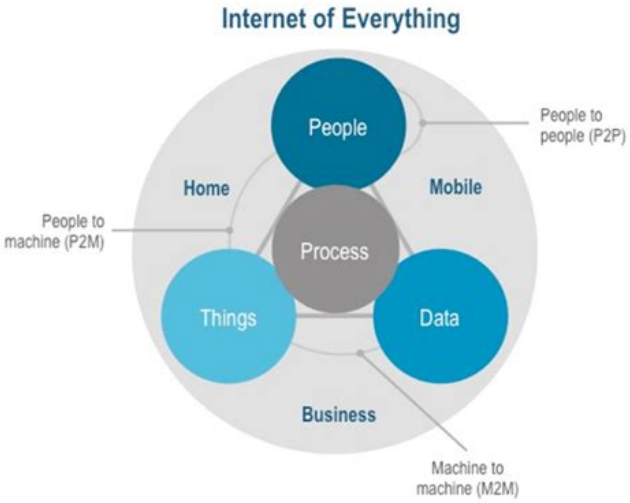

Figure 11: Shows how things are connected using IIOT

Cloud[iii]

According to NIST Special Publication 800-145 (September 2011), "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."

Essential Characteristics:

1. On-demand self-service. A consumer can provision server time and network storage without human interaction at the service provider.
2. Broad network access. Capabilities are available over the network and accessed through mobile phones, tablets, laptops, and workstations.
3. Resource pooling. The service provider's computing resources are aggregated to serve multiple consumers using a multi-tenant model, with different physical and virtual resources. These resources are assigned and reassigned dynamically based on the demand.
4. Rapid elasticity. Capabilities can be automatically scaled rapidly to match the demand. This can seem to the consumer that the resources are without limits.
5. Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability.

Service Models:

6. Software as a Service (SaaS). The software can be accessed through a browser or an App while the bulk of the software and processing occurs on the Cloud. The SaaS provider defines the access and where the processing occurs. The consumer manages the allowable user specific application configuration settings.

7. Platform as a Service (PaaS). The service provider manages and controls the underlying cloud infrastructure including network, servers, operating systems, or storage. The consumer has control over the deployed applications and potentially the configuration settings for the application-hosting environment.
8. Infrastructure as a Service (IaaS). The consumer has control over operating systems, storage, and deployed applications; and limited control of select networking components.

Deployment Models:

9. Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
10. Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns. It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
11. Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
12. Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).

The Cloud enables the ubiquitous availability of data and secure exchange of data, information, and knowledge. It is a very flexible tool to provide a variety of solutions based on the need throughout all timeframes.

Big Data Mining

Big Data / Data Mining are terms used to reference analyzing data sets that are too large and/or are too complex for traditional tools.

Big Data is very useful in predictive analytics and user behavior analytics. Data sets are growing rapidly because of so many connected devices and so many measures that have not traditionally been possible.

Think of Big Data as connecting the dots to convert data into information and then information into knowledge which can drive actions and behaviors.

Machine Learning/Artificial Intelligence:

Machine Learning/Artificial Intelligence is the formal study of algorithms and statistical models that computer systems use to progressively improve performance of a specific task without specifically being programmed to perform that task. It is very useful in predictive analytics or decisions.

Framework for End to End in Situ Monitoring[iv]

This framework establishes common interfaces wrapped around network entities (e.g.; a mobile phone, part of a network, an entire network, or anything in between). This approach enables communication between networks. This allows for one network that appears to be attacking another network to communicate the Cyber Security threat and collaborate with the adjoining networks to identify and eliminate the Cyber Security threat. This approach a proactive methodology in conjunction with the traditional reactive monitoring techniques. This approach also allows for the solution to work regardless of which network components are used in a given network or adjoining networks. This approach also addresses the historical problem of No Fault Found (NFF) errors. This approach works well with other tools from the IT Industry (Agile, Bid Data, etc.). This monitoring would occur in a live network and not require a formal a lab environment. The tests and monitoring can begin with a small group of friendly testers and, then subsequently, get scaled up as appropriate. Concepts from the automobile industry (e.g. Lean, Statistical Process Control (SPC), continuous improvement, etc.) can also be used to help make the network more resistant to Cyber Security Threats. In addition, networks can collaborate to find the source(s) of Cyber Security threats by using this methodology.

Assuming a Fault->Error->Failure model in conjunction with utilizing a modular network element approach, a basic set of metrics can be monitored from an end to end perspective (e.g. error rate, junction temperature, memory utilization, etc.) in situ on an ongoing basis to determine, with a minimal number of resources, the basic health of the network. If a monitored value is determined to be outside of a tolerance or specification range, then additional metrics from a larger standard set of metrics list (active/passive/hybrid metrics) can be captured and reported to an automatically updated network health dashboard and technical resources that can evaluate, as well as permanently resolve, the issue(s). This would be a two-step process. The first step would be a short term solution to identify the root cause of the problem by catching it early enough to clearly see the initiating issue and fix the symptom. For example, for a software coding fault, the erroneous value can then be replaced with a known safe value as part of a fault tolerance mechanism to help the overall network be more fault-tolerant. If there is a hardware fault, then the appropriate action can be prompted (e.g. sharing the resource load if the processor temperature gets too high, using an alternative hardware resource if the voltage is unstable or within specification, but not within the defined tolerance range, correlating reliability data from chipsets or other components based on service time or use cases). The

longer term fix would be to remove it from the network and/or change the hardware or software design to prevent the problem from ever occurring again. The Fault->Error-> Failure model , along with this larger standard set of metrics list, will enable operators to proactively find patterns in the data which will help to identify the root causes of errors before they cascade into such large and complex issues that it becomes difficult to identify the root cause of the problem. This methodology can be useful in finding corner cases and subtle problems that would not normally have been found using traditional methods.

This model does not require an understanding of the techniques and methodologies being used inside the monitored network section. This model is analogous to the standard interface of an automobile. If you turn the steering wheel or apply the brakes and the vehicle does not turn or stop, then you know that you have a problem.

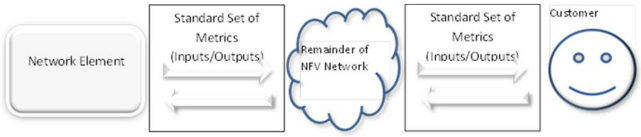

Figure 12: End To End Metrics (Including VNF, NFVI, and MANO Components)

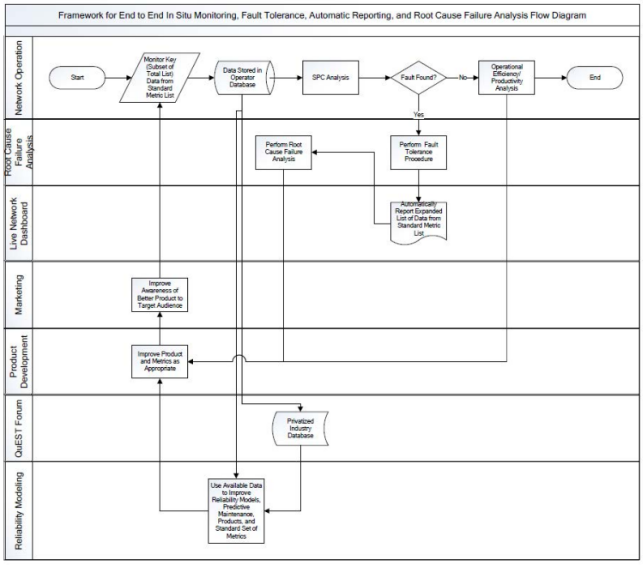

Figure 13: Process Workflow

Potential Extensions of IPC 1782, IPC 2581, and IPC 2591:

The role of exact traceability within an assembly operation provides the essential evidence with which to track the responsibility for any counterfeit or other quality issues related to incoming materials back to the source. To enable this to propagate through the supply-chain prior to materials arriving at the assembly site, the principles of ICP-1782 can be applied to material packaging and labelling, in a way that ensures that responsibility is taken for the materials at the time of packing, whether by an original manufacturer or distributor, that then cannot be tampered with prior to being received at the destination without clear evidence. IPC 2581's DFx (Design for Assembly, Manufacturability, and Assembly) can be matured for SMT/CCA. Because of the way IPC 1782 and IPC 2591 are structured, they can be easily extended and expanded into industries where the Electronics Industry has gone. Multiple companies have technologies that can find unique aspects of components by examining an image and storing only the unique aspects of that component, part, or product. This enables a unique tagging mechanism that can help secure the supply chain regardless of what happens to the components, parts, or products when they leave the site where they are produced.

Figure 13 shows some examples of how exact traceability information and knowledge can be used to eliminate risk of counterfeit materials.

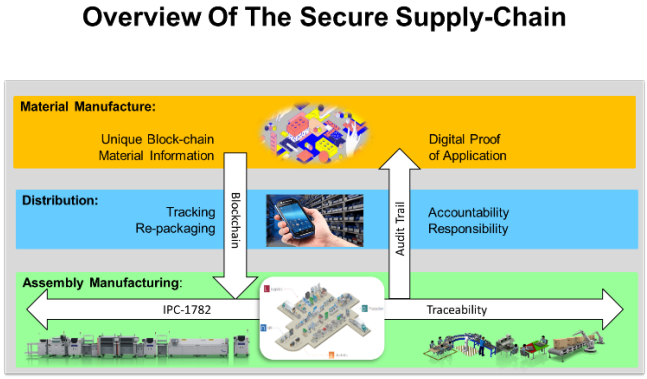

Figure 14 Summary of the Secure Supply Chain concepts outlined in this document.

The concept of the Secure Supply-Chain, when linked to exact traceability, will always allow the discovery of the responsible party for materials which may have been compromised for any reason. This is a powerful deterrent against counterfeit activities, as responsible parties must ensure that they are in control of materials, or face the consequences.

Conclusion:

In summary, IPC-1782, IPC 2581, and IIOT provide the information that impacts customer use, as well as, quality and reliability data. IPC's CFX enables this information to be easily collected and aggregated. Blockchain ensures those records do not change. Cloud enables easy access to that data. Big Data/Data Mining & Machine Learning/Artificial Intelligence converts the data contained in the cloud to actionable and useful information and subsequently into knowledge. Productivity can be significantly improved by implementing the technologies outlined in this paper, as well as, catch counterfeits and counterfeiters much closer in time and physical distance that ever before by taking a systematic approach to deal with surprise attacks. In addition to these key positive attributes, these tools enable a more robust opportunity to reduce the risk of Counterfeits and Cyber Security threats. Coupling these tools with the Framework

for End to End in Situ Monitoring described in Section 9.5 of ETSI GS NFV-REL 004 V1.1.1 (2016-04), a comprehensive Cyber Security solution can be created.

Figure 14 exemplifies how seemingly disconnected standardized data can be found to actually be connected using more and better data coupled with Big Data Tools.

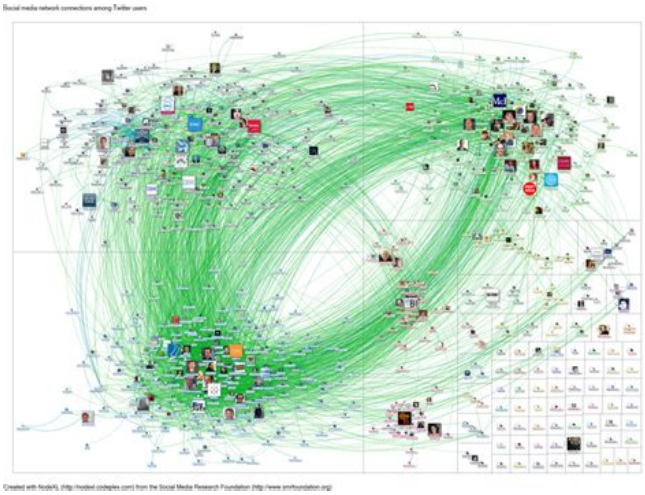

Figure 15: Connect, Collect, and Convert standardized data into actionable policies & procedures.

IPC-1782, IPC 2581, and IPC-2591 CFX are industry standards managed by task groups of industry volunteers which anyone can participate on. IPC wishes to encourage comments and participation. Please contact Chris Jorgensen (ChrisJorgensen@ipc.org) for more information on participation.

[i] (Shearon, 2019)
[ii] (Ford, et al., 2019)
[iii] (Mell, et al., 2011)
[iv] (Shearon, 2016)